EXHIBIT 18

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

SUPPLEMENTAL DECLARATION OF LOGAN LAMB

LOGAN LAMB declares, under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct:

Background and Credentials

1. My name is Logan Lamb. I am a cybersecurity researcher based in Santa Monica, California.
2. I have a Bachelor of Science and Master of Science degrees in computer engineering from University of Tennessee, Knoxville.
3. I have worked professionally in cybersecurity since 2010 when I started at Oak Ridge National Lab in the Cyber and Information Security Research group. In that position, I specialized in static and symbolic analysis of binaries, red-teaming prototype critical infrastructure, and de-identifying geospacial data.

4. I now work for the micromobility company Bird as a Senior Vehicle Security Engineer. In this role I protect Bird's fleet from both hardware and software-based hacking attempts.
5. I hereby incorporate my previous declaration as if fully stated herein. (Dock. 258, p. 126) In summary, in August 2016 I discovered serious vulnerabilities affecting elections.kennesaw.edu. The website was misconfigured so that it leaked confidential election data and the version of its content management system, Drupal, was out of date and vulnerable to a well-known exploit called drupageddon. An announcement from the Drupal security team on October 29, 2014 details how severe this vulnerability is, stating that if a vulnerable Drupal server was not updated within 7 hours of the announcement it should be assumed compromised. The Drupal software was still vulnerable in August 2016.[1]
6. Despite these warnings, KSU continued running the vulnerable version of Drupal until August, 2016, almost two years after patches were made available.
7. The server running elections.kennesaw.edu was taken offline on March 2nd, 2017 after KSU was notified a second time the server was still leaking sensitive election data. A forensic image of this server was created on March 6th, 2017 by the FBI.
8. The forensic image created by the FBI was provided to me in late December 2019 by CGG after I signed the protective order. After receiving a copy of the forensic image I confirmed the image was an exact copy of the one created by the FBI by comparing the SHA1 hash of the image to that provided to me.

[1] https://www.drupal.org/PSA-2014-003

9. On January 1, 2020 I began conducting a forensic audit of the provided image of the server running elections.kenessaw.edu.

10. The server image appears to contain all the files, databases, logs, and programs that were saved on the server when it was copied by the FBI on March 6th, 2017.

11. From my initial review of the server, I have four novel findings so far:

    a. There is evidence which suggests the server was compromised in December, 2014, well before the 2016 election.

    b. Access logs which would be critical to forensic work only go back to November 10, 2016, two days after the 2016 election.

    c. Election related files were deleted on March 2nd prior to taking the server offline and prior to the FBI creating an image.

    d. The version of BallotStation used by Georgia, 4.5.2!, is likely vulnerable to exploits affecting BallotStation 4.3.15 and beyond. Critical exploits affecting version 4.3.15 were documented in 2006.[2]

12. In the following sections I will expand on the above findings.

INDICATORS OF COMPROMISE

13. I found evidence which suggests a well-known attack named "shellshock" was successfully used against the server. The attack exploits a bug in common server software and gives the attacker full control of the computer. The Shellshock bug was so widespread, easy to exploit, and potentially devastating that when it was discovered in

[2] https://s3.amazonaws.com/citpsite/wp-content/uploads/2019/01/23191614/ts06full.pdf

September of 2014 it received significant media attention and dire warnings from the Department of Homeland Security.[3]

14. Despite those warning, CES did not patch the bug for months.

15. On December 2, 2014, while the KSU server remained vulnerable, a new user named "shellshock" was created on the server. I have created the below timeline of activity related to the shellshock user after fusing logging data from multiple sources. The timeline may not be complete:

16. 12/2/2014 10:45 – the user mpearso9 is modified using the Webmin console

    12/2/2014 10:47 - shellshock user created using Webmin console

    12/2/2014 10:49 - /home/shellshock/.bash_history last modified

    12/2/2014 11:02 - /home/shellshock/shellsh0ck file is deleted

    12/2/2014 11:06 - bash patched to version 4.2+dfsg-0.1+deb7u3 to prevent shellshock

    12/2/2014 11:40 - shellshock user disabled using Webmin console

17. The file named ".bash_history" is a kind of log that typically records all the commands a user executes. For this user, though, the file contained a single command to logout of the server. The single command to logout is suspicious since a file was created and deleted in the user's home directory, leading me to believe the ".bash_history" has been modified. This indicates to me that the "shellshock" user may have been hiding their activities.

18. When an attacker breaks into a server, it is common that they fix the bug that gave them access. That way, the attacker can keep control while keeping other would-be attackers out. That appears to be what happened on the KSU server. Just 20 minutes after the "shellshock" user was created, the logs show that the shellshock bug was patched.

[3] For a contemporary report, see https://www.nytimes.com/2014/09/26/technology/security-experts-expect-shellshock-software-bug-to-be-significant.html

19. The long unpatched software, unusual username, potentially modified command history, and near immediate patching of the shellshock bug are all strong pieces of evidence that an outside attacker gained access to the KSU server by exploiting the shellshock bug. There may still be other explanations. It is possible, for example, that a CES employee used a convoluted method of patching shellshock on December 2nd, 2014. Additional forensics need to be done to confirm the attack and determine what the attacker may have done with their access to the server.
20. If an attacker did indeed exploit the shellshock bug, then they would have had almost total control of the server including the abilities to modify files, delete data, and install malware.

MISSING LOGS

21. The website software, Drupal, was configured to maintain an access log. The access log contains all requests made to the webserver. If an attacker attempted to exploit drupageddon on the webserver then it would be apparent in the access log. However, the access log records on the server only go back to November 10, 2016, two days after the 2016 election.
22. The access logs will retain information indefinitely unless configured to automatically delete the oldest records based on age.
23. The missing logs could be vital to determining if the server was illegally accessed before the election, and I can think of no legitimate reason why records from that critical period of time should have been deleted.

FILES DELETED PRIOR TO FBI HANDOFF

24. In addition to the missing logs, there are also scores of files deleted on March 2nd, 2017. Some of the files appear to be unusually deleted and directly related to elections. Using the software "TestDisk,"[4] I was able to do a forensic search of the server image to find deleted files. I found many files deleted on March 2nd, 2017, just before the server was taken offline by the CES/KSU staff and the original server handed over to the FBI. I have not yet been able to determine what these deleted files were, but include the filenames below which I believe are related to elections and were deleted on March 2nd, 2017.:

2-Mar-2017 12:15 /countyfolders/Appling County/ExpressPoll/Proof/Ballots/1-90-NP-FB.pdf

2-Mar-2017 12:15 /countyfolders/Appling County/ExpressPoll/Proof/Ballots/1-90-NP-FB.pdf

2-Mar-2017 12:15 /countyfolders/Appling County/Proof/Ballots/1-90-NP-FB.pdf

2-Mar-2017 12:15 /countyfolders/Appling County/Proof/Ballots/1-90-NP-FB.pdf

2-Mar-2017 12:15 /countyfolders/do_not_use.php

2-Mar-2017 12:15 /countyfolders/do_not_use.php

2-Mar-2017 12:15 /countyfolders/Murray County/Proof/Audio/Murray Audio.zip

2-Mar-2017 12:15 /countyfolders/Murray County/Proof/Audio/Murray Audio.zip

GEORGIA MACHINES VULNERABLE TO KNOWN ATTACKS

25. In the server image I found three files which indicate the DREs in Georgia running BallotStation 4.5.2! are vulnerable to exploits affecting BallotStation 4.3.15:

    a. explorer.glb – this file is used as a backdoor to log into Windows CE on a DRE

[4] https://www.cgsecurity.org/wiki/TestDisk

b. BS_CE-TSR6-4-5-2!-DS.ins – a script which installs BallotStation on an Accuvote TS

c. BS_CE-TSX-4-5-2!-DS.ins – a script which installs BallotStation on an Accuvote TSX

26. I was able to extract BallotStation.exe from BS_CE-TSX-4-5-2!-DS.ins and confirm the DES key **F2654hD4** is in it. Because this encryption key has been publicly known for years, it means that anyone with access could have decrypted and altered data the DREs were meant to protect. That is, any encryption done by the DREs could have been trivially undone, and that important layer of security would have been totally ineffective.

27. The inclusion of this DES key indicates Georgia's version of BallotStation is likely very similar to version 4.3.15 which was extremely vulnerable to compromise. Like all the other data on the server, it was poorly secured could have been tampered with.

OTHER BAD PRACTICES

28. According to Michael Barnes' testimony, the server was supposed to be used for a few limited purposes. In reality, it appears elections.kennesaw.edu was the primary server for CES and was used for a wide variety of purposes. It includes copies of BallotStation to be installed on the DREs; databases of pollbook data for every registered voter in the state, including personally identifiable information; GEMS database files for numerous Georgia elections; training materials, and related machine and file passwords. The server even had installer files for Adobe Photoshop. A cursory review of these other files saved on the server show some other bad cybersecurity practices putting components and election files across the state at risk of intrusion and compromise.

29. The election and business files on this potentially compromised server appear to be of the type transferred between various parts of the State's election infrastructure over many years. As Dr. Halderman stated in his Declaration, "Although the KSU server itself was decommissioned in 2017, many of these potentially infected computers likely remain in use with the BMD-based system." (Doc . 692-3 ¶4). I agree with his conclusion.
30. It is unreasonable to assume that the new BMD election system and supporting infrastructure is not already potentially compromised or exposed to malware or given the broad range of election files on the CES elections.kennesaw.edu server.
31. Forensic analysis of the DRE components should be conducted to fully understand the nature of potential past compromises and to properly assess the current and future threat to the BMD system components and the systems that feed it, like the voter registration system.

I declare under penalty of perjury that the foregoing is true and correct and that this declaration was executed this 14th day of January, 2020.

LOGAN LAMB